

[Document Name] Abstract of the Disclosure

[Summary]

[Problem] A mobile node (MN) home address and HA (home agent) address may need to be dynamically changed when using prefix communication functions and HA address discovery functions, so methods for manually setting the IPsec SA security for encryption between the MN and HA are not practical in this environment. The current Mobile IPv6 protocol also has no function allowing recognition of the MN itself.

[Solution] Information on whether a prefix is distributable to a MN is held by a CA (certification authority). The server section of the HA allots prefix information to a MN approved by the CA. When the server section of the HA receives an IKE packet from the MN, the server section generates an IPsec SA after checking the prefix information in the server section. The server section allows an MN location registration request to fulfill the IPsec SA. The CA approves distribution of a prefix to the MN and verifies that the MN is genuine by generating an IPsec SA with the HA by utilizing the prefix distributed by the MN.

[Selected Drawing] Fig. 1